

UNCLASSIFIED



NORTH DAKOTA HOMELAND SECURITY ANTI-TERRORISM SUMMARY



The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

UNCLASSIFIED

UNCLASSIFIED

NDSLIC DISCLAIMER

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

QUICK LINKS

[NORTH DAKOTA](#)

[REGIONAL](#)

[NATIONAL](#)

[INTERNATIONAL](#)

[BANKING AND FINANCE
INDUSTRY](#)

[CHEMICAL AND HAZARDOUS
MATERIALS SECTOR](#)

[COMMERCIAL FACILITIES](#)

[COMMUNICATIONS SECTOR](#)

[CRITICAL MANUFACTURING](#)

[DEFENSE INDUSTRIAL BASE
SECTOR](#)

[EMERGENCY SERVICES](#)

[ENERGY](#)

[FOOD AND AGRICULTURE](#)

[GOVERNMENT SECTOR
\(INCLUDING SCHOOLS AND
UNIVERSITIES\)](#)

[INFORMATION TECHNOLOGY
AND TELECOMMUNICATIONS](#)

[NATIONAL MONUMENTS AND
ICONS](#)

[POSTAL AND SHIPPING](#)

[PUBLIC HEALTH](#)

[TRANSPORTATION](#)

[WATER AND DAMS](#)

[NORTH DAKOTA HOMELAND
SECURITY CONTACTS](#)

UNCLASSIFIED

NORTH DAKOTA

Medcenter says theft compromised patient information. A theft from an employee's unlocked vehicle has led to compromised patient information, Medcenter One said November 17. The hospital said a laptop and paper documents containing hearing-aid patient information were stolen from an employee's vehicle almost a month ago. A Medcenter One privacy officer said the laptop was password protected but contained about 650 names and dates of birth of hearing-aid patients, along with hearing tests. The laptop was 6 or 7 years old and has not been recovered; the bag containing the paper documents was found discarded on a trail not far from the scene of the theft a few days later. The recovered 11 charge forms contained names, dates of birth, addresses, phone numbers, insurance policy numbers and Medicare numbers, along with hearing diagnosis of 11 hearing-aid patients. The documents were used for billing purposes and were "not anywhere near their full patient record," said the privacy officer. Medcenter One is working with Experian, a credit reporting agency, and its ProtectMyID Alert program, to provide free credit monitoring to potentially impacted people who would like further identity theft follow-up on their personal information. Source:

http://bismarcktribune.com/news/local/crime-and-courts/medcenter-says-theft-compromised-patient-information/article_9c31e536-116d-11e1-8d40-001cc4c03286.html

Making safer dams. Work has started on a project to make two dams on the Red River south of Fargo-Moorhead, North Dakota safer, Fargo Valley News reported. The Christine and Hickson dams are being retro-fitted with stones. Work began near Christine the week of November 14. Crews will put field stones around the dam making it appear more like natural rapids. The changes will allow fish to pass by, while eliminating dangerous undertows. Other dams on the river — including the dams in Fargo — have already been upgraded. Source:

<http://www.valleynewslive.com/story/16059840/making-safer-dams>

Bond set for man charged with starting two apartment fires. A judge set bond at \$100,000 for a Fort Totten, North Dakota, man charged with setting fires at two apartment buildings in south Fargo November 13. The suspect is charged with two counts of attempted murder, aggravated assault, and endangering by fire. He is accused of injuring his cousin's two children before setting a fire in a bedroom. Police said he then started a fire at another apartment building a block away. Source: <http://www.kfgo.com/fm-headline-news.php?ID=0000005966>

Levee repairs underway. Levee repairs in North Dakota started on the eight sites where the levee was washed out or breached during the flood earlier in 2011, KXMB 12 Bismarck reported November 12. Ceres Environmental Services Inc. initiated their contract work November 10 at the Perkett ditch breach in Minot, North Dakota. The work at Perkett was expected to be completed the weekend of November 12 and 13. The three sites in the Country Club area will be complete late the week of November 21, weather permitting. Talbotts Nursery repairs will be started immediately upon completion of the Country Club sites. A U.S. Army Corps of Engineers site supervisor said the contractors will be working from sun up to sundown 7 days a week to complete the repairs. He said the final two sites in Renville County may take longer

UNCLASSIFIED

because they are different in nature, including damage to guard rails and pavement. Source: <http://www.kxnet.com/getArticle.asp?ArticleId=872586>

REGIONAL

Bagged salad recalled for E.coli. Thousands of bags of prewashed salad and romaine lettuce are being recalled over concerns that they may be contaminated by with E.coli, KSAZ 10 Phoenix reported November 18. Ready Pac Foods of Irwindale, California, shipped the salad to 15 states: Alaska, Arizona, California, Colorado, Hawaii, Idaho, Montana, Nebraska, Nevada, New Mexico, Oregon, South Dakota, Texas, Washington, and Wyoming. The affected salad has a use-by date of November 18. The recall includes 12 types of salad. Source:

http://www.myfoxphoenix.com/dpps/news/111811-Bagged-Salad-Recalled-for-E.coli_16008506

(Montana) Laid-off IT worker accused of hacking, crashing Missoula company's servers. When multiple computer servers crashed nearly simultaneously November 2 at Edulog, the Missoula, Montana, firm said it sought help from a former information technology (IT) administrator who had been laid off about a week earlier. Missoula County authorities allege it was that man who hacked into the computers in the first place, took the servers down and erased backup servers. The crash also affected Edulog's sister company, Logisys, which provides software for law enforcement, fire and emergency management services, including the Missoula County Sheriff's Office and the Missoula Police Department. The former IT administrator appeared in court November 19, charged with two counts of unlawful use of a computer. Both are felonies because the value of the property involved exceeded \$1,500. Bail was set at \$5,000. Edulog provides software for school bus routing and scheduling, GPS school bus tracking and systems that affect payroll for school districts. The Edulog servers crashed at 9 a.m., taking down Internet, e-mail, and other essential systems, plus client sites and information access for about 200 clients. A Edulog systems installation and help desk manager and his team told authorities most of the damage was done to configuration files, that were deleted, altered or overwritten in a way that would allow a person who had backup files to easily repair the problem. Source: http://missoulain.com/news/state-and-regional/laid-off-it-worker-accused-of-hacking-crashing-missoula-company/article_e8691d48-125d-11e1-bcc5-001cc4c002e0.html

(Montana; Wyoming) Pipelines owned by Conoco, Exxon at risk of failing. Federal safety regulators disclosed problems November 15 with oil and other hazardous liquid pipelines at seven major river crossings and hundreds of smaller crossings in Montana and northern Wyoming — problems that could put the lines at increased risk of failure. Problems found at the major river crossings must be fixed by spring 2012 or the companies that own them will face enforcement actions, according to an official from the U.S. Department of Transportation (DOT). That includes pipelines crossing the Missouri, Musselshell, Gallatin, Tongue, and other rivers that are owned by three companies: Exxon Mobil, CHS, and ConocoPhillips. Some repairs are under way, company officials said. Many of the pipelines were installed decades ago in shallow trenches just a few feet beneath riverbottoms. Erosion caused in part by record flooding has since exposed the lines or left them buried under minimal cover. The

UNCLASSIFIED

UNCLASSIFIED

consequences of a line failing was highlighted by an Exxon Mobil pipeline break in July that spilled 1,000 barrels of crude into the Yellowstone River, fouling dozens of miles of riverbank. The DOT official said he instructed his inspectors to take a similar look at pipelines elsewhere in the West. The most detailed information has been collected since the Yellowstone spill for Montana and portions of northern Wyoming within the Missouri River basin. More than 170,000 miles of pipelines carrying oil, refined petroleum, and other hazardous liquids crisscross the United States, crossing some 35,000 streams, rivers, and other water bodies, according to the DOT. Source: <http://fuelfix.com/blog/2011/11/16/pipelines-owned-by-conoco-exxon-at-risk-of-failing/>

(Wyoming) Latest EPA tests find high levels of groundwater benzene, other chemicals in Wyo. gas field. The U.S. Environmental Protection Agency (EPA) said it has found high levels of benzene and other chemicals in the latest groundwater samples from a community within a gas field. A variety of chemicals and high levels of methane turned up in two wells drilled specifically to test for pollution in the central Wyoming community of Pavillion. The carcinogen benzene measured as high as 50 times the EPA limit, according to a report released at an EPA public meeting November 9 in Pavillion. Elevated levels of diesel- and gasoline-grade organic compounds also were found. Meanwhile, the EPA has sampled 42 domestic water wells to date, finding methane in 10 wells and a chemical called 2-butoxyethanol phosphate in nine. So far the EPA is not speculating about where the pollution originated, but plans to release a summary of findings later this month. Source: <http://www.therepublic.com/view/story/18ba23e292874c96b8fa6a178f5922cd/WY--Pavillion-Contamination/>

NATIONAL

6 killed as storms sweep across South. Search teams combed through rural South Carolina early November 17 after a storm swept through the Southeast, killing at least six people and causing injuries in several states. At least three people died and five others were taken to hospitals after a November 16 storm hit York County, according to the sheriff's office. Two people died when a home collapsed late November 16 in Davidson County, North Carolina, according a spokesman with the county's emergency operations center. A sixth person died in Forsyth County, Georgia, when a tree fell on a car, the fire department said. Downed trees, damaged homes and buildings, and power outages were reported across Alabama and Georgia. The North Carolina governor confirmed one death in the state. An apparent tornado south of Winston-Salem damaged "multiple structures," according to North Carolina emergency management. Four people were injured in Mississippi, according to the National Weather Service. Homes were also reported damaged near Jones, Mississippi. A possible tornado demolished homes and vehicles near Opelika, Alabama. Alabama's Lee County received "significant reports of damage," said a public information officer with the county emergency management. "We've got reports of damage at an apartment complex, structures at a lake, mobile homes and trees down," she said. Earlier November 16, a suspected tornado in Louisiana's Tangipahoa Parish moved a home with four people inside off its foundation. Source: <http://www.cnn.com/2011/11/17/us/severe->

UNCLASSIFIED

UNCLASSIFIED

[weather/index.html?eref=rss_topstories&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+rss/cnn_topstories+\(RSS:+Top+Stories\)](http://weather/index.html?eref=rss_topstories&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+rss/cnn_topstories+(RSS:+Top+Stories))

J&J starts removing toxins from baby products. Johnson & Johnson has begun removing two harmful chemicals from its iconic baby shampoo and other baby products in the United States, Bloomberg reported November 16. An international coalition of consumer and environmental groups had pressed the company since May 2009 to remove the toxins from all personal care products, including Johnson's Baby Shampoo. Two weeks ago, the Campaign for Safe Cosmetics was emboldened after finding the New Jersey-headquartered health care giant had removed the two chemicals from products in several other countries. But in the United States, the products contain trace amounts of potentially cancer-causing chemicals. Johnson & Johnson now says it expects to remove formaldehyde-releasing preservatives from baby products within about 2 years, and is reducing traces of the other chemical. Source: <http://www.businessweek.com/ap/financialnews/D9R22IIG0.htm>

INTERNATIONAL

Romanian authorities cuff NASA hack suspect. Romanian authorities arrested a 26-year-old suspected of breaking into NASA's systems, causing damages estimated at \$500,000 in the process. The suspect was arrested November 15 in Cluj by officers from the Romanian Directorate for Investigating Organized Crime and Terrorism who were investigating a string of break-ins starting in December 2010 that were traced back to Romania. The means used or the motive for the attack remains unclear, but NASA is a frequent target of hacking attacks and almost as frequently a target of cybercrime prosecutions. Source: http://www.theregister.co.uk/2011/11/17/romania_nasa_hacker_charged/

BANKING AND FINANCE INDUSTRY

Fake bank site spreads malware. On November 18, the Office of the Comptroller of the Currency (OCC) issued a warning about HelpWithMyBank.com, an illegitimate Web site feigning to offer consumer information about bank accounts and loans. Once visited, the HelpWithMyBank.com URL directs users to a legitimate consumer information site, HelpWithMyBank.gov, attempting to convince users they are connecting to a legitimate site, according to the OCC. But connecting to the fake site before the redirect is believed to expose consumers to malware. Source: http://www.bankinfosecurity.com/articles.php?art_id=4257

SEC halts scam touting access to pre-IPO shares of Facebook and Groupon. The Securities and Exchange Commission (SEC) November 17 filed an emergency enforcement action to stop a fraudulent scheme targeting investors seeking stock in Internet and technology companies like Facebook and Groupon in advance of a public offering. The SEC alleges a Florida man and several other individuals carried out the scam using a newly minted hedge fund named The Praetorian Global Fund. They falsely claimed the fund and affiliated Praetorian entities owned shares worth tens of millions of dollars in privately-held companies expected to soon hold an initial public offering (IPO). Taking advantage of investor interest in pre-IPO shares that are

UNCLASSIFIED

UNCLASSIFIED

virtually impossible for company outsiders to obtain, the man and others solicited funds and gave investors a false sense of comfort their money was protected by telling them an escrow service was receiving their money. In reality, according to the SEC's complaint filed in federal court in Manhattan, the man and his cohorts never owned the promised pre-IPO shares. Three men were each actively involved in providing false documents and information to broker-dealer representatives in pitching their clients to invest in the Praetorian entities. They raised at least \$12 million from investors across the country during the past 15 months. Source:

<http://www.sec.gov/news/press/2011/2011-245.htm>

Federal financial fraud prosecutions tumble to lowest level in 20 years. Financial criminals are facing the lowest number of federal prosecutions in at least 20 years, according to a new report. The government has filed 1,251 new prosecutions against financial institution fraud so far this fiscal year, according to the Transactional Records Access Clearinghouse at Syracuse University. If the same pace holds, federal attorneys will file 1,365 such cases by the end of the year — the lowest number since at least 1991. The report, compiled from Justice Department data gleaned through the Freedom of Information Act, considers crimes involving crooked mortgage brokers, bank executives with something to hide, and accounts hiding illegal activity. The expected volume of prosecutions by the end of 2011 would be 2.4 percent smaller than that of last year, 28.6 percent thinner than that of 5 years ago, and less than half the amount from a decade ago. The number of federal bank fraud cases has slipped every year since 1999.

Source: http://latimesblogs.latimes.com/money_co/2011/11/federal-financial-fraud-prosecutions-tumble-to-lowest-level-in-20-years.html

IRS security deficiencies may put taxpayer data at risk. Information security failings are making it impossible for the U.S. Internal Revenue Service (IRS) to get its financial house in order and could be putting taxpayers' sensitive information at risk, according to a financial audit of the agency by the Government Accountability Office (GAO) released November 10. Deficiencies in information security continued to constitute material weaknesses in the IRS's internal control over the 2010-2011 fiscal year, as the IRS made meager progress addressing security concerns identified in previous audits. The GAO estimates the IRS corrected only 15 percent of the 105 previous security related recommendations from previous reviews. Past audits have revealed the IRS has difficulty maintaining control over and access to automated systems and software it uses to process financial transactions, produce internal and external financial reports, and safeguard related sensitive data. The "IRS was limited in its ability to provide reasonable assurance that ... proprietary financial and taxpayer information was appropriately safeguarded," the GAO found. According to the audit, the GAO claims material weaknesses in security limited the IRS's ability to reasonably ensure financial statements are fairly presented in conformity with generally accepted accounting principles, that financial information relied upon by management in day-to-day decision making is current, complete, and accurate, and that proprietary data being processed by automated systems is appropriately safeguarded. "These issues increase the risk of unauthorized individuals accessing, altering, or abusing proprietary IRS programs and electronic data and taxpayer information," the report states.

Source: http://threatpost.com/en_us/blogs/irs-security-deficiencies-may-put-taxpayer-data-risk-111411

UNCLASSIFIED

SEC charges UBS with faulty recordkeeping related to short sales. The Securities and Exchange Commission (SEC) November 10 charged UBS Securities LLC for inaccurate recording practices when providing and recording "locates" to customers seeking to execute short sales. UBS settled the enforcement action by agreeing to pay an \$8 million penalty, and retain an independent consultant. According to the SEC's order instituting settled administrative proceedings, UBS employees routinely recorded the name of a lender's employee even when no one at UBS had contacted the employee to confirm availability. The SEC's investigation found UBS employees sourced thousands of locates to lender employees who were out of the office and could not have provided any information to UBS on those days. "UBS permitted its employees to create records that do not accurately convey the basis upon which its employees granted locates," the director of the SEC's New York Regional Office said. The SEC's investigation found that since at least 2007, UBS's "locate log" that records the locates it granted "inaccurately portrayed which locates were based on electronic feeds or direct confirmation with specific lenders. UBS's practices obscured inquiry into whether UBS had a reasonable basis for granting locates, and created a risk of locates being granted based on sources that could not be relied upon if shares were needed for settlement." Source: <http://www.sec.gov/news/press/2011/2011-240.htm>

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

(Idaho) FDA issues warning to International Isotopes. The U.S. Food and Drug Administration (FDA) sent a warning letter to International Isotopes, a radiochemical product manufacturer based in Idaho Falls, Idaho, due to violations of Current Good Manufacturing Practice regulations, HealthImaging.com reported November 11. In the letter dated October 26, the FDA said many violations in the production of Sodium Iodide I-131 solution were discovered during a July inspection. The violations included: all appropriate identity tests were not performed on each batch of incoming components; there was no established written procedure for calibration of pipettes, scales and radioisotope calibrators used in the manufacture of Sodium Iodide I-131; software used in batch production had not been validated; and written procedures for storage, handling, labeling and other processes lacked sufficient detail. In addition, the letter said International Isotopes was manufacturing Sodium Iodide I-131 solution, classified as a "new drug," without an approved FDA application. But the FDA said it would allow continued production of the solution while the manufacturer corrects the violations. "This decision is consistent with FDA's commitment to take action against marketed unapproved drugs without imposing an undue burden on patients," an FDA district director said. International Isotopes previously responded to the inspection observations in August, but the response lacked sufficient corrective actions, according to the warning letter. Source: http://www.healthimaging.com/index.php?option=com_articles&view=article&id=30404:fda-issues-warning-to-international-isotopes

COMMERCIAL FACILITIES

Bands of Occupy protesters march in several cities as movement enters 3rd month.

Thousands of Occupy Wall Street demonstrators took to the streets around the United States November 17 to mark 2 months since the movement's birth and signal they are not ready to quit, despite the breakup of many of their encampments by police. At least 175 people were arrested in New York. More than 1,000 demonstrators gathered near the New York Stock Exchange and staged sit-ins at several intersections. The demonstration around Wall Street failed to disrupt operations at the stock exchange, but brought taxis and delivery trucks to a halt. Police said four officers went to a hospital after a demonstrator threw some kind of liquid in their faces. Many demonstrators were carrying vinegar as an antidote for pepper spray. One man was taken into custody for throwing liquid, possibly vinegar, into the faces of several police officers, authorities said. Helmeted police broke up some of the clusters, but most of the crowd re-assembled in Zuccotti Park, where the encampment that served as the unofficial headquarters of the Occupy movement was broken up by police earlier in the week. Organizers in New York said protesters would fan out across Manhattan later in the day and head into the subways, then march over the Brooklyn Bridge. Police in Los Angeles arrested 23 people. About 500 sympathizers, many of them union members, marched in downtown Los Angeles between the Bank of America tower and Wells Fargo Plaza. In Albany, New York, about 250 protesters from Buffalo, Rochester, and other encampments arrived by bus to join a demonstration in a downtown park. Police in Portland, Oregon, closed a bridge in preparation for a march there, and later detained more than a dozen people who sat down on the span. Demonstrations were also planned or under way in such cities as Washington, D.C., St. Louis, Las Vegas, and Portland, Oregon. In Dallas, police evicted dozens of protesters near city hall, citing health and safety reasons. Eighteen protesters were arrested. Two demonstrators were arrested and about 20 tents removed at the University of California, Berkeley. City officials and demonstrators were trying to decide what to do about an encampment in Philadelphia, where about 100 protesters were ordered November 16 to clear out immediately to make way for a plaza renovation at city hall. Source: http://www.washingtonpost.com/national/occupy-movement-plans-day-of-action-in-nyc-nationwide-officials-bracing-for-thousands/2011/11/17/gIQA BMISTN_story.html?hpid=z2

(Maryland) Hours after Md. mall shootings, police fatally shoot suspect after exchange of gunfire. A man suspected of killing two people outside a Hanover, Maryland, shopping mall November 12 was fatally shot hours later in an exchange of gunfire with Prince George's County police officers, authorities said. A Prince George's police spokesman said the suspect was killed after emerging from a District Heights home with two guns. He said the suspect shot one officer in the torso with a shotgun, but the officer was expected to survive. Six officers were believed to have opened fire. The spokesman said the man killed was suspected in the fatal shooting hours earlier of two people in the parking lot of Arundel Mills Mall in Hanover. Prince George's police went to the home based on information and tips received by Anne Arundel police. Source: http://www.washingtonpost.com/local/police-investigate-whether-man-shot-by-pg-officer-is-suspect-in-shootings-at-md-mall/2011/11/12/gIQA lczLFN_story.html?tid=pm_local_pop

COMMUNICATIONS SECTOR

AT&T restores Northeast wireless data service after disruption. AT&T, the second-largest U.S. mobile carrier, said it restored data service to wireless customers in New York and elsewhere in the Northeast after a disruption earlier November 21. "Some mobility customers were unable to connect to data services briefly early this morning," an AT&T spokesman in Atlanta said. "The issue was resolved." The disruption, which affected mobile e-mail and Internet access, began at 6:14 a.m. in New York, according to AT&T's customer-service department November 21. The Dallas-based company began an investigation into the issue, which customer-service representatives described as a "service degradation." Some customers using Apple iPhones and Research In Motion BlackBerrys said they noticed a loss of e-mail service shortly after 6 a.m., and by 7:45 a.m. some of those AT&T customers reported e-mail began to work again. Source: <http://www.businessweek.com/news/2011-11-21/at-t-restores-northeast-wireless-data-service-after-disruption.html>

Earthlink follows Blackberry with widespread e-mail outages. First Blackberry, now Earthlink. The \$730 million Internet service provider experienced "severe" e-mail outages all day November 14, the company announced. Its online support chat system was overloaded, telling callers the next available support staff would be available within the next 70 minutes. The company's Twitter page was not updated with any news about the outages, but Earthlink subscribers were tweeting about the outage since 11 a.m. Source: <http://www.forbes.com/sites/kenrapoza/2011/11/14/earthlink-follows-blackberry-with-widespread-email-outages/>

CRITICAL MANUFACTURING

Smith & Wesson recalls Thompson Center Venture rifles. Smith & Wesson is recalling all Thompson Center Venture rifles manufactured before October 28, according to the company, Guns.com, and the Minneapolis Star-Tribune November 14. During an internal technical review, Smith & Wesson identified a condition that may exist with the sear supplied with some rifles that would allow the rifle to fire without the trigger being pulled. The new announcement broadens the recall announced by Smith & Wesson November 8. Any unintended discharge of a firearm has the potential to cause injury or death, and the company asked consumers to stop using the affected rifles until the sear is inspected for the defect. Smith & Wesson is offering a free inspection and repair of the rifles. Source: <http://www.startribune.com/sports/blogs/133810523.html>

DEFENSE/ INDUSTRY BASE SECTOR

Nothing Significant to Report

EMERGENCY SERVICES

Sprint customers first to receive wireless emergency alerts. Thanks to Sprint, the Federal Emergency Management Agency (FEMA) will now be able to broadcast wireless emergency alerts to cell phones for the first time; the move allows FEMA, the U.S. President, the National Weather Service, or local and state emergency officials to broadcast warning messages and safety information through text messages. In addition, emergency officials can geo-target alerts so that only subscribers in a specific area receive messages. For instance, an emergency alert can be sent only to cell phones at a stadium event, or residents in specific neighborhoods can be targeted in the case of a wildfire or tornado. When the system is activated, targeted cell phones will receive a 90-character text alert with a distinct vibration cadence and audio tone similar to the sound of radio and television emergency alerts. Sprint is still testing the system, and later this year, the company will work with federal officials to conduct the first test of alerts to mobile phones in New York City. Source:

<http://www.homelandsecuritynewswire.com/sprint-customers-first-receive-wireless-emergency-alerts>

(California) Calif. prison guard pleads in phone-smuggling case. A California prison guard has pleaded guilty to a federal crime stemming from allegations he took bribes from inmates to smuggle tobacco and cell phones. The U.S. attorney's office in Sacramento said the guard faces a maximum sentence of 20 years in prison after pleading guilty November 14 to a single count of honest-services wire fraud for taking payments in exchange for sneaking tobacco and telephones into prison. He was charged with federal crimes because the allegations included money crossing state lines. He was indicted on six charges alleging he took nearly \$16,000 to smuggle the contraband into the California Correctional Center in Susanville. He acknowledged the single charge under a plea agreement. Sentencing is scheduled for February 6. Source:

<http://www.sacbee.com/2011/11/14/4054560/calif-prison-guard-pleads-in-phone.html>

ENERGY

Cyber-security of power grid in 'near chaos,' report says. The cybersecurity of the North American power grid is "in a state of near chaos," according to report by Pike Research, a consulting group monitoring the industry's transition to wireless digital technologies, the Ottawa Citizen reported November 15. The group's white paper revealed a \$60 smart phone application can bypass security measures and allow direct communications between the phone and some industrial control systems (ICS) that regulate breakers, relays, feeders, and the flow of electricity. As the industry evolves from largely isolated systems to a grid built around interoperable, digital technologies, security jitters are rising. Many ICS have lifespans of 30 years, and mitigation and compensation measures to help them mesh with the newer technologies are creating additional weak links and vulnerabilities. The installation of "smart meters" to improve electricity distribution efficiency is also a potential gateway for attacks. In a rush to install a patchwork of fixes to address potential cybersecurity gaps and with some utilities investing in compliance minimums rather than full security, "the attackers clearly have the upper hand," said the report. Source:

UNCLASSIFIED

<http://www.ottawacitizen.com/technology/Cyber+security+power+grid+near+chaos+report+says/5715327/story.html>

(Nebraska) Officials report diesel supplies short in Nebraska. Gasoline and diesel shortages at fuel terminals in the Upper Midwest have forced fuel truck drivers to sit in line for hours, waiting for fuel to arrive via pipeline. Other truck drivers have seen diesel prices rise, nearing \$4 a gallon in Nebraska, and passing that in the Dakotas. One of the two fuel terminals south of Lincoln, Nebraska, has not had diesel for at least a month. When a supply comes in to the other, it runs out in a few hours. A spokesman for Magellan Midstream Partners, which owns one of the terminals, blamed the shortage on a combination of factors. There has been extremely high demand for diesel at the terminals in the northern part of his company's system. Much of the demand comes from growth in the region's oil and natural gas industry, but there is also seasonal demand from farmers bringing in their crops. Other reasons include export demand, and refineries switching over to winter blends. Source: http://www.cbsnews.com/8301-505245_162-57322952/officials-report-diesel-supplies-short-in-nebraska/

FOOD AND AGRICULTURE

(California) Organic Pastures milk quarantined, recalled. Organic Pastures raw dairy products are being recalled statewide in California, and are subject to a quarantine order by the California State Veterinarian, Food Safety News reported November 16. The quarantine order came following notification by the California Department of Public Health that five children were infected, from August through October, with the same strain of E. coli O157:H7, the state said. Under the recall, all Organic Pastures raw dairy products with the exception of cheese aged at least 60 days must be pulled immediately from retail shelves. Until further notice, Organic Pastures may not produce raw milk products for the retail market. The order also affects Organic Pastures raw butter, raw cream, raw colostrum, and a raw product labeled "Qephor," state public health officials said. The children who are ill are residents of Contra Costa, Kings, Sacramento, and San Diego counties. Source: <http://www.foodsafetynews.com/2011/11/quarantine-order-against-organic-pastures-recall-underway/>

Recall: Plastic in Wegmans mashed sweet potatoes. Wegmans Food Markets said 4,000 pounds of its mashed sweet potatoes were being recalled because of possible contamination with pieces of white plastic, the Associated Press reported November 12. The Rochester, New York-based grocery chain said the sweet potatoes packaged in 24-ounce plastic trays were sold between September 22 and November 9 in dairy departments at its stores in New York, Pennsylvania, New Jersey, Virginia, Maryland, and Massachusetts. They were recalled by supplier Orval Kent Foods of Wheeling, Illinois. Wegmans said four consumers complained about the plastic bits. Source: <http://www.chicagotribune.com/news/local/chi-ap-ny-wegmansrecall,0,5916954.story>

Badia recalls 3,800 pounds of packaged pine nuts for possible salmonella contamination. Badia Spices in Miami recalled 3,800 pounds of packaged pine nuts November 10, because they

UNCLASSIFIED

UNCLASSIFIED

may be contaminated with salmonella, the Fort Lauderdale Sun-Sentinel reported November 11. The nuts were sold in retail stores in Florida, and four other states from June to October, Badia said. Badia repackaged the nuts purchased in bulk from a New Jersey firm that recalled them this month after several illnesses. Samples contained salmonella bacteria. Source: <http://www.wptv.com/dpp/news/state/badia-recalls-3,800-pounds-of-packaged-pine-nuts-for-possible-salmonella-contamination>

(California) Potential botulism in black bean tortillas. United Natural Foods (UNFI) is recalling certain types of Gentes Foods Gordita Black Bean Tortillas because they have the potential to be contaminated with *Clostridium botulinum*, Food Safety News reported November 11. The latest recall was the second in 2 days for the company, which recalled certain types of Divina stuffed olives and Tabatchnick Yankee Bean Soup November 9. In each case, the company said the recalls were due to a lack of temperature control during the distribution process. UNFI said it inadvertently subjected the recall items to temperature ranges above those directed by the manufacturer. Source: <http://www.foodsafetynews.com/2011/11/potential-botulism-in-black-bean-tortillas/>

South Africa finds E. coli in 22 tons of Irish cheese. At South Africa's eastern port of Durban, a shipment of 22 tons of cheddar cheese sent from Ireland will be destroyed because it was contaminated with *E. coli*, Food Safety News reported November 14. South African milk producers immediately asked their government to put a temporary ban on Irish dairy products. The cheddar cheese shipment from Ireland was found to be "too risky for human consumption" after it docked at the South African port. The cheese was shipped in 25-kilo blocks and was said to have enough bacteria to cause food poisoning in anyone consuming it. Durban port officials said the cheese would be returned to the Irish shipper who would then have the responsibility of destroying the product. Source: <http://www.foodsafetynews.com/2011/11/e-coli-found-by-south-africa-in-22-tons-of-irish-cheese/>

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

US satellites compromised by malicious cyber activity. On at least two occasions, hackers took over U.S. satellites and targeted their command-and-control systems, a report by the U.S.-China Economic and Security Review Commission revealed November 16. The incidents involved two Earth observation satellites. While it may be difficult to trace who hacked the satellites, U.S. officials acknowledged the incidents had to come from a nation power. U.S. officials cannot clearly trace the incidents to China, but the report released by the Congressionally mandated commission noted Chinese military writings made reference to attacks on ground-based space communications facilities. The report noted some of the malicious cyber activity targeting the satellites involved NASA's Terra EOS satellite being targeted in June 2008, and again in October 2008. The June incident resulted in the satellite being interfered with for 2 minutes, and the October incident lasted at least 9 minutes. The report noted that in both instances, "The responsible party achieved all steps required to command the satellite but did not issue

UNCLASSIFIED

UNCLASSIFIED

commands.” NASA confirmed the incidents in a separate statement. The report noted the Landsat-7 satellite operated by the U.S. Geological Survey experienced similar interference and events in 2007 and 2008, but added the entity behind that incident did not achieve the ability to control the satellite. The report mentions the serious implications the intrusions could have on the satellite systems, particularly if they were directed against more sensitive systems such as military or communications satellites. Source:

<http://abcnews.go.com/blogs/politics/2011/11/us-satellites-compromised-by-malicious-cyber-activity/>

(District of Columbia) Oscar Ramiro Ortega-Hernandez charged with attempt to assassinate Obama. An man accused of firing two shots at the White House the week of November 7 has been charged with attempting to assassinate the U.S. President or his staff. The man, from Idaho Falls, Idaho, made his first court appearance before a federal magistrate in Pittsburgh November 17, 1 day after he was arrested at a western Pennsylvania hotel. He will be taken back from a federal court in Pittsburgh to face the charges in Washington, D.C. Source:

http://www.washingtonpost.com/blogs/crime-scene/post/oscar-ramiro-ortega-hernandez-charged-with-attempt-to-assassinate-obama/2011/11/17/gIQAZC9BVN_blog.html

Employees' Droids among biggest government cyber menaces. In 2012, agencies should worry about hackers attacking the growing number of federal employees toting their own iPhones and Droids to work, according to a forecast of 2012's greatest cyber dangers compiled by M86 Security Labs. On November 15, the network security firm released its annual predictions of the top computer threats to business and government organizations. At federal agencies, the biggest targets are likely to be employee-owned devices, a department's own public Web site, and cloud services. Agencies without policies to manage security on an employee's smartphone or tablet may have no way of protecting government data from online viruses, according to the research. Even devices that are centrally managed could be vulnerable to intrusions in 2012 because mobile antivirus software has not yet matured, the report said. Source:

http://www.nextgov.com/nextgov/ng_20111115_9168.php

(California) Alleged gunman shot by cops at UC Berkeley is dead. An alleged gunman who was shot by police on the University of California, Berkeley campus died. A campus spokesman said the man was an undergraduate transfer student who was attending classes at the Haas School of Business. Police officers tracked the suspect into a Haas computer room November 15 after an employee reported seeing a man with a gun. During the confrontation, the suspect was shot. He was taken to an Oakland hospital, where he later died, the campus spokesman said. Source:

http://www.msnbc.msn.com/id/45314276/ns/us_news/#.TsO6hXJinus

(Hawaii) HPD bomb unit, HFD hazmat team respond to suspicious package at UH Manoa. Some classes at the University of Hawaii (UH) at Manoa were disrupted November 13 after the discovery of a suspicious package. The FBI said it was the fifth such package found on campus in the past week. UH campus security shut down Maile Way near East-West Road as the Honolulu Fire Department haz-mat team prepared to examine a suspicious package left in the loading dock of the Paradise Palms Cafe. The discovery forced the evacuation of the eatery, Hamilton

UNCLASSIFIED

UNCLASSIFIED

Library, and three classroom buildings. Authorities said the outside of the package had similar handwriting to the four that were found on the Manoa campus November 7. The others did not contain anything harmful or threatening. More than three hours after the initial call, the all-clear was given. The package containing papers was harmless. Source:

<http://www.hawaiinewsnow.com/story/16036339/fbi-investigates-suspicious-package-at-uh>

(District of Columbia) GAO: FBI facilities face security challenges. Dispersion of Federal Bureau of Investigation (FBI) staff in annexes throughout the National Capital Region creates security challenges, according to a Government Accountability Office (GAO) report. The report found "the FBI's headquarters facilities — the Hoover Building and the headquarters annexes — do not fully support the FBI's long-term security, space and building condition requirements." It said FBI security officials indicated to GAO staffers they had "some security concerns — to varying degrees— about some of the headquarters annexes." These concerns include proximity of non-FBI tenants to FBI employees performing sensitive operations, lack of control over common areas, and the fact that "security at the annexes is primarily handled by contract guards, local police or the FBI's internal police force, the FBI police, depending on the location and circumstances." With its employees dispersed throughout the National Capital Region and many of them housed in the aging and inefficient Hoover Building, which was constructed prior to current Interagency Security Committee Standards [ISC] governing security countermeasures, GAO said, "the FBI is under pressure to find an alternative that will meet its security, space, and building condition requirements. Any alternative will take years to implement and is likely to cost over a billion dollars." Source:

[http://www.hstoday.us/index.php?id=95&tx_ttnews\[tt_news\]=19996&cHash=27a86d6b82b8494a621a8058cd6bf189](http://www.hstoday.us/index.php?id=95&tx_ttnews[tt_news]=19996&cHash=27a86d6b82b8494a621a8058cd6bf189)

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Android malware, up 472 percent, seeing fastest growth ever. As Android market share has shot up in recent months, so has the volume of malware designed for the mobile platform. There has been a 472 percent increase in Android malware samples in the last 3 months alone, according to research from Juniper Networks. While September saw a 28 percent jump in malware samples, the numbers for the months of October and November are trending upwards and might translate into the fastest growth of Android malware the platform has ever seen. October's numbers saw a 110 percent increase over September, a 171 percent increase from what was collected up to July 2011, the company said on its Global Threat Center blog. Juniper's research found the bulk of Android malware is behaving one of two ways: 55 percent was disguised as spyware while 44 percent hijacked phones and utilized a SMS trojan to send expensive messages without the user's knowledge. Source:

http://threatpost.com/en_us/blogs/android-malware-472-percent-seeing-fastest-growth-ever-111511

Researchers find new way to hide messages in VoIP. Researchers have devised a new scheme for hiding secret data within VoIP packets, making it possible to carry on legitimate voice conversations while stolen data piggybacks on the call undetected, making its way to thieves on

UNCLASSIFIED

UNCLASSIFIED

the outside. Called transcoding steganography or TranSteg, the method calls for setting a larger-than-necessary payload space in VoIP packets and using the extra room to carry covert messages. In their experiment, the researchers could send 2.2MB of covert data in each direction during an average 7-minute phone call. Source:

http://www.computerworld.com/s/article/9221832/Researchers_find_new_way_to_hide_messages_in_VoIP

Duqu targeted each victim with unique files and servers. The creators of the Duqu malware that penetrated industrial manufacturers in at least eight countries tailored each attack with exploit files, control servers, and booby-trapped Microsoft Word documents that were different for each victim, according to research published November 11. Two of the drivers the sophisticated, highly modular rootkit used in one attack showed compilation dates of 2007 and 2008, the Kaspersky Lab expert and author of the report said. If the dates are genuine, they suggest the Duqu architects may have spent the past 4 years developing the malware. The Duqu version examined in the report was recovered by the Sudan Computer Emergency Response Team from an undisclosed company the attackers targeted in advance. Like attacks on other targets, it was launched using a booby-trapped Word document with content tailored to the receiving organization, and exploited a previously unknown vulnerability in the kernel of all supported versions of Microsoft Windows. Source:

http://www.theregister.co.uk/2011/11/11/duqu_analysis/

sn3Ak3r hacks social network and leaks 57,000 credentials. Social network FindFriendz.com was attacked by An0nym0us sn3Ak3r, a member of t34m t!g3R, and credentials on 57,000 members were stolen. E Hacking News reported the social network's Web site lost the information as a result of an SQL injection attack that took advantage of a common vulnerability. The hacker published only a small part of the stolen data, but he claimed he would make the rest available for anyone who requests it. Source:

<http://news.softpedia.com/news/sn3Ak3r-Hacks-Social-Network-and-Leaks-57-000-Credentials-234240.shtml>

NATIONAL MONUMENTS AND ICONS

(Ohio) Ohio national forest halts sale of drilling rights. The U.S. Forest Service has decided to hold off on selling drilling rights in Ohio's only national forest so officials there could explore potential impacts from the process known as fracking. The Wayne National Forest supervisor said in a statement November 15 that more than 3,000 acres have been withdrawn from a natural gas and oil lease sale scheduled for December 7. Hydraulic fracturing, or fracking, is a horizontal drilling technique for gas that uses chemical-laced water to break up shale deep underground so trapped gas is released. Local leaders from areas near the forest in southeast Ohio had protested the lease sale, saying they feared a fracking accident could harm the forest. The supervisor said the forest would bring together experts to study fracking's possible effects above ground. Source: <http://www.wkyc.com/news/article/215066/3/Ohio-national-forest-halts-sale-of-drilling-rights>

UNCLASSIFIED

UNCLASSIFIED

(Illinois) **Copper sword stolen from statue at Lincoln's Tomb.** Thieves stole a 3-foot-long copper sword atop Abraham Lincoln's Tomb in Springfield, Illinois, in what is believed to be the first theft at the site in more than a century, the Associated Press reported November 12. An employee noticed the week of November 7 the sword was cut from a statue of a Civil War artillery officer, the Springfield State Journal-Register reported November 12. Officials believe the sword was stolen sometime between September and early November. The rest of the statue was unharmed. A spokesperson for the Illinois Historic Preservation Agency said officials plan to fix the statue. Source: <http://www.chicagotribune.com/news/local/breaking/chi-copper-sword-stolen-from-statue-at-lincolns-tomb-20111112,0,7231200.story>

POSTAL AND SHIPPING

Nothing Significant to Report

PUBLIC HEALTH

Shortage Of ADHD drugs has parents, doctors scrambling. The scarcity of attention deficit hyperactivity disorder (ADHD) medications is a problem faced by an untold number of children and adults with the disorder, National Public Radio reported November 21. ADHD is not the only disorder for which drugs are in short supply. Many medications are increasingly in shortage, leading the U.S. President to issue an executive order October 31 to help unsnarl the supplies. But the problem has been concentrated on intravenous medications used in hospitals, and cancer chemotherapy agents. However, for reasons that are unclear, in recent months the hard-to-get drugs include ADHD medications such as Adderall. Last week, methylphenidate, the active ingredient in Ritalin and generic equivalents, was officially declared in shortage. Nobody knows how many people are affected by the shortages. Up to 15 million children and adults are thought to have ADHD, and more than half of children with the disorder take medication for it. Source: <http://www.wbur.org/npr/142571217/shortage-of-adhd-drugs-has-parents-doctors-scrambling>

TRANSPORTATION

American Eagle Airlines fined \$900,000 for lengthy tarmac delays. The U.S. Department of Transportation (DOT) said November 14 it fined a regional affiliate of American Airlines \$900,000 for keeping hundreds of passengers cooped up for hours on planes in Chicago earlier in 2011, a clear warning to airlines that similar incidents will not be tolerated. American Eagle Airlines had tarmac delays of more than 3 hours on 15 flights arriving at O'Hare International Airport May 29, the department said in a statement. A total of 608 passengers were aboard the delayed flights. The airline must pay \$650,000 of the fine within 30 days, the department said. Up to \$250,000 can be credited for refunds, vouchers, and frequent flyer mile awards provided to the passengers on the 15 flights, as well as to passengers on future flights that violate the 3-hour rule, the department said. The department implemented a new rule in April 2010 limiting tarmac delays on domestic flights to 3 hours. After that, airlines must either return to a gate or provide passengers who wish to leave planes with some other means of safely getting off.

UNCLASSIFIED

UNCLASSIFIED

Airlines that violate the rule can be fined as much as \$27,500 per passenger. The rule has since been extended to international flight delays, which are capped at 4 hours. Source:

http://www.huffingtonpost.com/2011/11/14/american-eagle-airlines-fined_n_1092050.html

WATER AND DAMS

Hacker says he had no intention of harming plant, only proving a point. A hacker posted diagrams of a Harris County, Texas community's sewer system online to show how easy it is to infiltrate the system, the Associated Press reported November 19. The mayor of South Houston told the Houston Chronicle that no harm was done, but the DHS and FBI are investigating. A hacker identified as "pr0f" posted the diagrams. The mayor said the plant's control system has since been taken offline. The hacker told the newspaper by e-mail that it was easy to access South Houston's online infrastructure diagrams. He said he had no intention of harming the plant, but that he wanted only to prove a point. South Houston is a city of 16,000 people in the Houston area. Source:

<http://www.therepublic.com/view/story/da45f624b6434f2989d9d082a47e4957/TX--Sewer-System-Targeted/>

(Michigan) EPA: Enbridge spilled 1.1M gallons of oil, much more than estimated. The extent of the July 2010 oil spill that contaminated the Kalamazoo River was nearly 40 percent greater than previously estimated, according to the U.S. Environmental Protection Agency (EPA). Enbridge Energy, the company whose pipeline ruptured near Marshall, Michigan in July 2010, has claimed since the incident occurred that it lost an amount of heavy crude oil ranging between 819,000 and 843,000 gallons. However, the EPA's Web site was updated November 16 to report 1,139,569 gallons of oil were recovered during cleanup efforts. The Web site also indicated more work is needed to clean up submerged oil, implying that even more oil remains to be found. The Web site said the EPA "has identified pockets of submerged oil in three areas covering approximately 200 acres that require cleanup." One of those sites is in the Mill Pond in Battle Creek, and another lies within and east of Ceresco. The third is in Morrow Lake. The EPA reported 15.7 million gallons of oil and water have been collected and disposed of since the cleanup began, involving work by 783 personnel. At the height of the cleanup in September, more than 2,500 EPA, state, local and Enbridge personnel and contractors were working along 35 miles of river and shoreline, according to the EPA Web site, which added that the cleanup effort continues to have more than 500 people deployed to the region. Source:

<http://www.battlecreekenquirer.com/article/20111117/OILSPILL/111170311/Kalamazoo-River-oil-spill-EPA-Enbridge-Battle-Creek?odyssey=tab|topnews|text|Frontpage>

NORTH DAKOTA HOMELAND SECURITY CONTACTS

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: **North Dakota State and Local Intelligence Center:** 866-885-8295 (IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 **State Radio:** 800-472-2121; **Bureau of**

UNCLASSIFIED

UNCLASSIFIED

Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168

UNCLASSIFIED